TRABAJO DE FIN DE MÁSTER

Título:

PLAN ESTRATÉGICO EDUCATIVO DE SEGURIDAD Y PRIVACIDAD EN LA RED PARA ALUMNOS Y DOCENTES EN LOS CENTROS DE ENSEÑANZA

Apellidos: **BRAGADO PÉREZ**

Nombre: **MIGUEL**

Titulación: Máster en Formación del Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanza de Idiomas

Especialidad: **TECNOLOGÍA**

Director/a: **MARC ANTONI SOLER CONDE**

Fecha de lectura**: 25/6/2014**

Índice

1. INTRODUCCIÓN

Las nuevas tecnologías de la información, han irrumpido con fuerza en los centros de enseñanza, facilitando a los docentes su labor en materia de gestión académica en el centro así como la posibilidad de crear innovadores y creativos de modelos enseñanza que impacten en el alumno. Los alumnos también son participes de este auge tecnológico que va en aumento con el paso de los años donde se han visto inmersos en la vorágine tecnológica que estamos viviendo.

Con todo ello, se tiene que tener presente el correcto uso de las tecnologías de la información, ya que una mala utilización de la misma puede conducir potencialmente: al aislamiento y al descuido de las relaciones sociales, de las actividades académicas, de las actividades recreativas, de la salud y de la higiene personal; Según informe de Investigación por el consorcio europeo EU NET ADB del 2013, financiado por la unión europea, sobre conductas adictivas a Internet entre los adolescentes europeos (1).

Para ello, es necesario que los docentes sean conocedores de dicha problemática que puede ser causada mediante un mal uso referente a las nuevas tecnologías de la información. De modo que el docente en su centro educativo tenga el conocimiento necesario para aconsejar y ayudar a sus alumnos o detectar posibles conflictos y problemas relacionados con las nuevas tecnologías de la información.

De lo que se denota, que los centros necesitan profesionales formados en esta materia que puedan lograr hacer frente, adelantarse o en su defecto minimizar los posibles conflictos en los que sus alumnos se pueden ver involucrados debido determinados comportamientos en internet.

Es de vital importancia que el alumno sea consciente de los peligros que puede acarrear un mal uso de la red, donde en la actualidad, es frecuente ver noticias incluso a diario, acerca de casos de ciberacoso, sustracción de información o pérdida de la privacidad.

El docente y por ende el centro de enseñanza, pueden ser una gran ayuda en la formación del menor fomentando el buen uso de las tecnologías de comunicación.

Teniendo en cuenta que, una competencia básica metodológica del currículum de la educación secundaria obligatoria es el "*Tratamiento de la información y competencia digital*" (2) en la que el alumno debe tener una actitud crítica y reflexiva en la valoración de la información disponible respetando las normas de conducta acordadas socialmente para regular el uso de la información

El aprendizaje ético adquirido en el centro de enseñanza debe lograr por tanto, el respeto, aprendiendo a convivir estableciendo vínculos basados en la comprensión a los demás. Incluso si esta convivencia es en una comunidad virtual, el alumno deberá conocer cómo comportarse, respetar a los demás y ser consciente de los peligros y riesgos a evitar.

1.1 ANTECEDENTES

El uso de las tecnologías de la información, se ha convertido en algo imprescindible y de uso diario tanto para docentes como alumnos.

En la actualidad, un docente puede disponer de libros digitales para sus alumnos, pizarras electrónicas en el aula, proyectores, o el uso de entornos virtuales educativos como la herramienta moodle citando tan solo algunos ejemplos. No sorprende encontrarse un aula en la que los alumnos poseen cada uno un ordenador portátil perfectamente equipado y conectado a la red de internet por medio de uno de los servidores del centro de enseñanza. A su vez, es diario el uso de herramientas multimedia para la realización de ejemplos de ejercicios de las diferentes unidades didácticas o la realización de trabajos mediante procesadores de texto.

Lo mencionado, es algo que a día de hoy nos puede parecer habitual, pero donde no hace tanto tiempo no existían las posibilidades tecnológicas de las que se disponen en la actualidad.

La informática ha ido y sigue creciendo cada día más, en la cual no se ha sabido gestionar dicho crecimiento, dejando internet sin ningún tipo de restricción o gestión de contenidos de acceso a un menor. Con ello tampoco se ha sabido ofrecer una "cultura tecnológica" en esta materia, a la sociedad actual y ahí es donde entran alumnos y docentes en juego.

Ante el no control del tratamiento de la información, familia y docentes, deben conocer cómo prevenir de un mal uso en esta materia a los alumnos del centro de enseñanza. Del mismo modo, que los alumnos deben conocer cómo actuar ante diferentes situaciones en la vida, deben conocer cómo actuar en un mundo tecnológico en el que la destrucción de la reputación de una persona o citando otro caso, la aparición de un trastorno de la personalidad provocado por dicho mal uso puede acarrear graves problemas. Si estos problemas son detectados a tiempo, o evitados mediante un entendimiento de la implicación que puede tener según qué decisión o actitud se tome en la red, en muchos casos se podrán entonces evitar conflictos y resolver situaciones que de otro modo no sería posible.

Con el citado auge de las nuevas tecnologías, aparecen las denominadas redes sociales, las cuales han pasado a formar parte de una sociedad que pretende globalizar el uso de las mismas. Lo cual como en tantos casos tiene sus ventajas y sus inconvenientes que en este caso serán analizados ya que como adelanto citaré que un mal uso de las redes sociales puede tener graves consecuencias. Como la tendría a su vez la pérdida de información personal, de un determinado dispositivo como el teléfono móvil que también ha pasado, de ser un pequeño teléfono para llamar y enviar mensajes, a un pequeño ordenador con su sistema operativo integrado.

Sin duda, son grandes avances tecnológicos los citados, en los cuales, se deberán tomar las medidas necesarias, donde como se ha comentado se necesita una "cultura tecnológica" por parte de la sociedad y es por ello que el centro de enseñanza debe cumplir con su función en este marco, facilitando a los alumnos aquellos conceptos, enseñanzas y directrices que logren una correcta capacitación en el buen y correcto uso de las tecnologías de la información a fin de evitar cualquier riesgo que pueda derivar en un grave problema.

1.2 OBJETIVO DEL TFM

El objetivo del trabajo final de máster *"Plan estratégico educativo de seguridad y privacidad en la red para alumnos y docentes en los centros de enseñanza",* es la realización de un plan estratégico educativo que logre garantizar la seguridad y privacidad de alumnos y profesores en materia de seguridad tecnológica.

El plan estratégico tendrá como objetivo lograr que alumnos y profesores del centro docente posean los conocimientos y las técnicas de medidas de seguridad necesarias para un uso responsable y seguro en la red.

A fin de lograr el objetivo, partiendo desde un escenario totalmente nuevo, se propondrá un plan estratégico que se podrá implantar en un centro educativo, el cual se beneficiará de la incorporación de las medidas de seguridad tecnológicas necesarias para la correcta convivencia de la comunidad educativa.

Algunos de los objetivos definidos en el trabajo final de máster, tienen la siguiente finalidad concreta:

- Garantizar la seguridad y privacidad en la red del centro docente.
- Establecer la formación necesaria a profesores y alumnos en materia de seguridad informática.
- Prevenir el ciberacoso a profesores y alumnos: (Ciberbaiting, Ciberbullying, Grooming…).
- Implantar medidas y protocolos de seguridad tecnológica en el centro docente.
- Conocer las técnicas y herramientas necesarias para la privacidad y seguridad en las redes sociales.
- Resolver conflictos que dañan la privacidad de los miembros de la comunidad educativa.

1.3 BENEFICIO PARA LOS ALUMNOS Y FAMILIAS

La propuesta del trabajo final de máster, aporta un beneficio para los alumnos y por ende para las familias al poder adquirir en el centro de enseñanza conocimientos tan importantes en la era actual como el uso responsable y seguro de las tecnologías de la información y comunicación. De este modo los padres de los alumnos se benefician que sus hijos sean capaces de evitar situaciones conflictivas en la red como se detallarán a lo largo del trabajo.

La implementación por tanto de un plan educativo en el centro de enseñanza referente a la seguridad y privacidad en la red para los alumnos, proporciona a los padres tranquilidad y una ayuda para sus hijos referente a cómo hacer un uso correcto, responsable y seguro de las tecnologías de la información.

1.4 BENEFICIO PARA LOS DOCENTES

El plan propuesto logra otorgar a su vez los conocimientos necesarios a los docentes para formar a sus alumnos en el uso seguro y responsable de las TIC. De modo que mediante el plan de seguridad y privacidad en la red realizado, los docentes obtengan conocimientos y recursos específicos en la materia para poder trabajar sobre estos temas en el aula.

Se benefician de unos conocimientos en materia de privacidad y seguridad en la red, que en la actualidad pueden formar parte de problemáticas o conflictos en determinados alumnos. Y si no se conoce la posible causa o tipología del problema, es complicado para un docente poder hablar con las familias para tratar de ofrecer una solución o en otro caso tratar de evitar que el problema se produzca ayudando al alumno a prevenirlo.

1.5 ESTRUCTURA DEL DOCUMENTO

El documento está estructurado del siguiente modo:

En primer lugar se presenta el problema, con su definición, contexto y los agentes implicados. Se realiza un estudio general de los principales riesgos de la red, divididos en privacidad y en posibles conflictos de relación que aparecen entre los alumnos los cuales trascienden a la Red.

A continuación se realiza una aplicación práctica de las medidas de seguridad referentes al tratamiento de la información de los ficheros del centro de enseñanza.

Se realiza la descripción de la solución aportada con los contenidos de seguridad y prevención en la red propuestos que deben conocer alumnos y docentes, así como el establecimiento de protocolos de actuación sencillos y eficaces para el uso adecuado de las nuevas tecnologías en los centros escolares.

Se proponen medidas de seguridad avanzadas a implantar desde el departamento de SI/TI del centro de enseñanza y se finaliza el documento con un decálogo de indicaciones referentes a las tecnologías de la información para el plan de convivencia del centro educativo.

Al final del documento se muestra la bibliografía y las páginas web consultadas.

Citar que en el trabajo, la solución propuesta, nace como fruto de mi experiencia en seguridad informática como graduado en ingeniería informática habiendo trabajado en multinacionales líderes en el sector de la seguridad informática Y de la experiencia en las prácticas realizadas en el máster donde he apreciado el desconocimiento general de la problemática en materia de seguridad en la red. Tanto por alumnos como por docentes, donde no he apreciado en el propio centro de enseñanza ningún tipo de medida en la red capaz de asegurar la privacidad de los usuarios, y la seguridad de conexiones a páginas web apropiadas para los alumnos. Evitando la posibilidad de conexión en aquellas páginas no apropiadas para los alumnos.

2. DEFINICIÓN Y CONTEXTO GENERAL DEL PROBLEMA

Las nuevas tecnologías de la información han llevado consigo la aparición de fenómenos hasta su llegada desconocidos como el *ciberbullyng* o acoso escolar a través de la red en el que se dan a su vez otras situaciones como las usurpaciones de identidad, calumnias, amenazas e injurias entre otras.

De otro modo, pueden suceder otro tipo de situaciones que provocan conflictos y requieren de un tratamiento especial como pueden ser todos aquellos peligros que aparecen por la falta de privacidad en internet, que ponen de manifiesto la necesidad de poder afrontarlos con éxito si se han producido o conocer como intervenir para evitarlos. En este marco podemos citar problemas como el *grooming* produciendo el acoso sexual a través de internet o el *sexting* mediante el envío de imágenes de contenido sexual o exhibicionista.

El centro de enseñanza debe ser idóneo para formar a los alumnos en el uso responsable y seguro de las tecnologías de la información y comunicación, aprendiendo a relacionarse de modo correcto también dentro de la red.

En el centro de enseñanza donde he realizado las prácticas, he notado en falta, materiales y recursos específicos para los profesores y educadores referentes a la seguridad y privacidad en la red con los cuales poder formar a los alumnos y reflexionar sobre la importancia del correcto uso seguro de las tecnologías de la información. Materiales con los que conocer o tener algún tipo de noción referente a los problemas psicológicos más comunes que causa la red en los menores, con tal de estar en disposición de ofrecer ayuda al alumno. De modo que el docente en su centro educativo tenga el conocimiento necesario para aconsejar y ayudar a sus alumnos, o detectar posibles conflictos y problemas de personalidad derivados de un mal uso de las nuevas tecnologías de la información.

Los alumnos, deben conocer cómo hacer un uso seguro y responsable de las nuevas tecnologías, conociendo las consecuencias que puede tener un uso inadecuado, el cual los expone diferentes riesgos. Riesgos, que he separado en dos áreas para un mejor tratamiento adecuado a la problemática:

- Privacidad en internet
- Conflictos de relación en la red

En referencia a la privacidad, se hace mención, en aquellos riesgos derivados de la falta de privacidad en las redes. En cuanto a los conflictos de relación en la red, trata aquellos riesgos que se producen en la red y trascienden como pueden ser las redes sociales donde los alumnos comparten su información sin conocer los riesgos que determinados comportamientos pueden acarrear.

Se denota, por consiguiente, que los centros necesitan que sus profesionales, los educadores sean conocedores y estén formados en esta materia para que puedan lograr hacer frente, adelantarse o en su defecto minimizar los posibles conflictos en los que sus alumnos se pueden ver involucrados debido determinados comportamientos en internet los cuales definidos como “adicciones psicológicas sin substancia” (Mark Griffths, 1995) (3).

3. ESTUDIO DE LOS PRINCIPALES RIESGOS

Se realiza un estudio de los principales riesgos y conductas que crean adicción en la red por parte de los adolescentes.

Referente a las adicciones por parte de los adolescentes, citar en primer término, el excesivo uso de internet, que afectan al rendimiento académico como argumenta M,Chóliz (2012)(4*) "Internet es una herramienta tecnológica que favorece las relaciones interpersonales pero en los casos de abuso puede suponer un problema y concretamente en los menores de edad afecta a su vida cotidiana y al rendimiento escolar"*.

Se aprecia un aumento en el tiempo que los adolescentes dedican a internet para comunicarse. Un 95 % usa internet cada día para comunicarse y casi uno de cada cuatro adolescentes (22,7%) pasa más de tres horas al día realizando esta actividad (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2013) (5).

Podría decirse que "han cambiado" los videojuegos y la televisión por la comunicación por internet (internet como vía de comunicación más que como una vía de información).

Y es que precisamente España, es el país europeo con mayor porcentaje de adolescentes en riesgo de desarrollar conductas adictivas, con un 21,3% según el estudio del consorcio europeo EU NET ADB del 2013(1), de ahí radica la importancia de adquirir estrategias que les impidan caer en estos problemas que pueden dar como resultado el absentismo y el fracaso escolar por el uso excesivo de internet.

El perfil con más probabilidades de caer en trastornos según el estudio mencionado, son los adolescentes de entre 16 y 17 años cuyos padres tienen un nivel educativo medio-bajo, con una evidente falta de comunicación en el entorno familiar. Edades de alumnos que cursan estudios de educación secundaria obligatoria y bachillerato que implica una menor dedicación de tiempo a estudiar, lo cual repercute en el rendimiento en clase.

Las redes sociales, o la adicción a los juegos en línea, son a su vez causa de la mencionada adicción a internet, Sánchez Burón y Álvaro Martín (2012) (6) comprobaban como entre el 80% y 90% de los adolescentes en edad escolar utilizaban las redes sociales, citando que España según estudio realizado es uno de los países donde están menos concienciados con los posibles peligros. Referente al estudio del consorcio europeo EU NET ADB del 2013(1) en España, un 39% de los adolescentes pasan más de dos horas al día en las redes sociales, tiempo que en este caso sitúa la media de la Unión Europea en un 23%, lo que pone a España por encima de la media siendo un dato que muestra el gran tiempo que nuestros adolescentes dedican a las redes sociales incluso superior a la media europea.

Los juegos en línea por su parte son otro peligro potencial derivado de la red que repercute directamente en los resultados académicos del alumno, debido al gran número de horas que transcurre jugando en línea por la red a los diferentes juegos en línea por parte del adicto a dichos juegos.

En este contexto algunas de las señales de alarma son el progresivo aislamiento, abandono de responsabilidades, problemas de atención y concentración, una variedad de síntomas físicos como consecuencia del mantenimiento prolongado de una postura y alteraciones del sueño que provocan que el alumno se encuentre siempre cansado en el centro. En España encontramos jóvenes y adolescentes adictos a los juegos online, que sufren trastornos de conducta y otros efectos psicosociales negativos derivados de este problema y que requieren tratamiento

La casuística, es probable que aumente por el desconocimiento en muchos casos de las familias en materia tecnológica, no siendo conscientes del problema que internet puede causar en la formación de sus hijos y el impacto tan negativo que puede acarrear en un futuro inmediato; Ya no solamente son riesgos a nivel académico sino personal poniendo en riesgo la vida de los adolescentes, en casos que no provienen de la adicción a internet pero si derivado del uso del propio uso la red, como el ciberacoso (ciberbullying).

El ciberacoso, una forma de invadir el mundo de la víctima de forma continua, disruptiva y sin consentimiento utilizando las posibilidades que ofrece la red de Internet, es una muestra perfecta del desconocimiento del peligro del menor en internet, donde en España.

Los chicos realizan más conductas en la red de riesgo de ciberacoso, el 44,5% de los chicos y el 37,1% de las chicas han aceptado dos o más veces como amigo o amiga en la red a una persona desconocida, y 38,3% de los chicos y 30,2% de las chicas han respondido en dos o más ocasiones a un mensaje en el que le insultan u ofenden. (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2013) (5).

No evitado en la mayoría de casos por el menor, precisamente por la ignorancia y no haber sido asesorado ya sea en un centro de enseñanza o por la propia familia de cómo actuar en estos casos. En primer lugar evitando el contacto con ciberacosadores mediante pautas básicas a seguir y en segundo lugar perdiendo el miedo a denunciar siendo conscientes de que el no denunciar y el miedo es lo que hace que prosperen este tipo de delitos.

El docente y el centro de enseñanza, por tanto pueden ser una gran ayuda en la formación del menor fomentando el buen uso de las tecnologías de comunicación. Es clave para evitar este tipo casuística enseñar a los alumnos cómo estar seguros en la red, debido al crecimiento exponencial de la tecnología y su facilidad de acceso como la que ofrecen los teléfonos móviles. El 2,5% de los menores confiesa haber sido objeto de ciberacoso a través del smartphone por parte de otros menores (7).

El acoso sexual o “grooming” es una conducta de alto riesgo para el adolescente en la cual el adolescente debe ser consciente del peligro que puede acarrear, donde según los datos el adolescente no está formado en el modo en que debe evitar estas posibles conductas de alto riesgo ya que un alto porcentaje contacta con extraños a través de la red. *El 20,6% de las chicas y el 25,6% de los chicos, han quedado con un chico o una chica que se ha conocido a través de internet. El 8,6% de las chicas y el 15,6% de los chicos han respondido a alguien desconocido que le ofrece cosas (5)*. Los datos dejan en evidencia, la mencionada falta de formación por parte del adolescente donde es necesario que tomen conciencia del peligro real que pueden suponer determinados comportamientos.

Con la información aportada, se llega a la conclusión de la necesidad de una formación específica para los alumnos en seguridad en la red, que bien puede impartirse en las diferentes tutorías con el alumnado o por medio de conferencias en el propio centro de enseñanza. En el trabajo se propondrán mecanismos para que docentes y alumnos sean capaces de comprender los riesgos de internet a fin de evitar o tratar de minimizar lo máximo posible dichos riesgos.

Debiendo seguir una línea maestra que garantice que los menores están preparados para garantizar su seguridad en la red y tratar de evitar reproducir aquellos comportamientos que pueden poner en riesgo el futuro personal y académico del alumno.

4. DESCRIPCIÓN DE LA SOLUCIÓN

4. 1. APLICACIÓN DE PRIVACIDAD Y NORMAS DE PROTECCIÓN DE DATOS EN LOS CENTROS DE ENSEÑANZA

Desde mi experiencia en las prácticas realizadas del máster en el centro de enseñanza, he apreciado desconocimiento por parte de alumnos y docentes en el área de seguridad y protección de datos. No he encontrado un plan de convivencia del centro adaptado al uso de las Nuevas tecnologías, en el cual se debería dejar constancia de la aplicación de privacidad y normas de protección de datos en el centro.

La constitución española de 1978 garantiza *"el derecho al honor, a la intimidad personal y familiar y a la propia imagen"* (art. 18.1 CE). A su vez, cita que "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*" (art. 18.4 CE).

Los centros de enseñanza por consiguiente, deben ser conscientes de que sus alumnos son titulares de los derechos fundamentales que se deben respetar:

- El derecho a su intimidad, recogido en el art. 18 de la Constitución Española (8).
- El derecho a la protección de sus datos de carácter personal, consagrado en la Sentencia del Tribunal Constitucional 292/2000.(9)

La Ley Orgánica de Protección de Datos (10), nace con el objetivo de "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*" (art. 1 LOPD), siendo aplicable "*a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"* (art. 2 LOPD).

Con la entrada en vigor de la Ley Orgánica 15/1999(8) de Protección de datos de carácter personal se establece la obligación de tener que notificar a la Agencia de Protección de Datos los ficheros con datos de carácter personal registrados en soporte físico, así como inscribirlos en el Registro General de Protección de Datos. Y el deber de crear una documentación de seguridad en la que aparezcan los artículos del Reglamento de Medidas de Seguridad de los ficheros automatizados que tengan incluidos datos de carácter personal como se aprobó en el Real Decreto 994/1999 del 11 de Junio.

En el marco legal vigente actual referente a la protección de datos aparece:

- **Constitución Española**
- **LOPD**: Ley orgánica 15/1999 de 13 de diciembre
- **Directiva 94/46/CE del Parlamento Europeo y del Consejo:** hace referencia en cuestiones relacionadas con el tratamiento de los datos
- **Agencia Española de Protección de Datos**: Agencia pública encargada del cumplimiento de la protección de datos
- **Reglamento 1720/2007 de Desarrollo de la LOPD**
- Ley 5/2002 de 19 de abril, de la **Agencia Catalana de Protección de datos**: realizan en el ámbito territorial de Cataluña, en las administraciones públicas, resoluciones de consultas, sanciones, inspecciones...

La Disposición adicional vigesimotercera de la LOE (11) establece que *"la incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad"*. Por lo cual, el hecho de la incorporación del alumno o la alumna al centro de enseñanza implica el consentimiento para el tratamiento de sus datos.

En los **centros de enseñanza pública** es necesario notificar los ficheros en el Registro General de Protección de Datos por medio de un responsable del fichero "*la obligación de notificación corresponderá al responsable del fichero, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*

Los ficheros tratados de un **centro docente concertado** deberán acogerse al régimen establecido para los ficheros de titularidad privada como se establece en el artículo 5.1.l del Real Decreto 1720/2007, por el cual se aprueba del Reglamento de desarrollo de la LOPD. Entendiendo como centro concertado tales los centros privados acogidos al régimen de conciertos legalmente establecido.
En cuanto a los centros privados concertados el fichero tendrá el mismo tratamiento que el régimen establecido para los ficheros de titularidad privada.

El centro de enseñanza necesita según el reglamento de la Protección de datos (1720/2007), analizar en referencia a los ficheros registrados un documento de seguridad, donde designaremos a los responsables de los ficheros y de seguridad, de los administradores y usuarios de seguridad.

Para ello, se documentan los responsables de cada fichero del centro de enseñanza del siguiente modo:

Figura 1.

FICHERO ALUMNOS:

Nombre y Apellidos	Cargo en el centro	Tipo de acceso	Alta	Baja
NOMBRE_USUARIO1				
NOMBRE_USUARIO2				

Respecto a las medidas referentes a los tipos de fichero, he realizado una serie de medidos de seguridad a adoptar por el centro de enseñanza para su correcto nivel de seguridad, tanto para la seguridad de los ficheros de nivel básico y nivel medio.

Citar que las medidas propuestas las he desarrollado desde mi experiencia en diferentes compañías donde he trabajado como Ingeniero en el área de Seguridad Informática

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS DE NIVEL BÁSICO DEL CENTRO DE ENSEÑANZA

1. Elaborar un documento de seguridad que recoja medidas técnicas y organizativas referentes a la normativa vigente de seguridad.

2. Registrar las incidencias: Tener a disposición un procedimiento para notificar y registrar las incidencias.

3. Funciones y obligaciones del personal: Definir y documentar las personas con acceso a los datos de carácter personal

4. Usuarios: Crear relación de los usuarios con acceso autorizado a los ficheros con datos de carácter personal, de los responsables de Seguridad y otras figuras que estipula la ley.

5. Gestionar los usuarios y contraseñas en la red. Cada empleado debe disponer de un usuario personal y contraseña para el acceso al sistema operativo de su equipo y a los servicios en por lo que se elaborará un procedimiento definido y documentado de asignación, distribución y renovación de códigos de acceso, no será superior a un año.

6. Creación de un sistema que permita añadir perfiles de acceso para asegurar que los usuarios únicamente tienen acceso a los datos y recursos necesarios para el desarrollo de sus funciones.

7. Realización de Backups diarios.

8. Dispositivos de almacenamiento: Se diseñaran mecanismos que hagan difícil su visualización/apertura.

9. Dispositivos portátiles: Tomar medidas de seguridad necesarias para este tipo de dispositivos.

10. Vigilancia de soportes: Impedir que a la documentación pueda acceder personal no autorizada.

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS DE NIVEL MEDIO DEL CENTRO DE ENSEÑANZA:

1. Identificación y autentificación de acceso: Crear un mecanismo que limite la posibilidad de intentar varias veces el acceso no autorizado al sistema de información por ejemplo mediante la creación de políticas del sistema operativo limitando el número de intentos desde una misma IP.

2. Realizar auditorías internas o externas al menos cada dos años.

3. Gestión de soportes y de documentación: Creación de un registro de entrada de soportes que facilite conocer el tipo de documento, la fecha y hora, el emisor, el número de documentos, el tipo de información que contenga, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

4. Control de accesos físico: Solamente el personal autorizado tendrá acceso a las ubicaciones donde se encuentren los equipos físicos de los sistemas de información.

5. Registro de incidencias: Deberán documentarse los procedimientos de recuperación de datos, indicando la persona que va ejecutar el proceso y los datos restaurados

El centro de enseñanza tiene que tener presente que existen ficheros especialmente protegidos con una protección más fuerte y que debe garantizar mayor seguridad, (art. 7 de la Ley Orgánica 15/1999) (8). En este contexto encontramos los siguientes ejemplos para el centro:

- Datos de origen racial de determinados estudiantes del centro de enseñanza
- Datos referentes al grado de minusvalía de algunos estudiantes del centro de enseñanza que requieren necesidades educativas especiales.
- Datos de determinados estudiantes del centro de enseñanza que tienen problemas de salud y les imposibilita hacer ejercicio físico.
- Datos referentes a la salud de los estudiantes del centro de enseñanza obtenidos en diferentes test realizados por los orientadores del centro.

4.2 FORMACIÓN EN LOS ALUMNOS PARA EL CORRECTO USO DE INTERNET

Se realiza una propuesta de formación de los alumnos del centro de enseñanza en el uso responsable y seguro en la red.

Se definen los riesgos y las conductas asociadas:

Figura 2

Riesgo	Conducta Asociada
Uso abusivo y adicción	Dependencia o uso excesivo Aislamiento social
Acceso a contenidos inapropiados	De carácter sexual Violento, racista o sexista Anorexia, bulimia o cuestiones estéticas Sectas o terrorismo Contenido que vulnere los valores en que se educa al hijo falso, inexacto o incierto
Interacción y acecho por otras personas y ciberbullying	Ciberbullying pasivo (ser acosado, insultado o amenazado por niños) Ciberbullying activo (acosar, insultar o amenazar a niños) Interacción / chat con desconocidos Tratar con adultos que se hacen pasar por niños Ser insultado por adultos Citarse a solas con desconocidos
Acoso sexual	Ser objeto de acoso sexual
Amenazas a la privacidad	Facilitar datos personales Que se difundan imágenes del alumno sin conocimiento. Que el alumno grabe y difunda imágenes inapropiadas.
Amenazas técnicas y/o malware	Virus Programa malicioso o espía Intrusión en cuentas de servicio web

Figura 2 *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres.(INTECO,2009) (12)*

El plan propuesto incluye que los docentes del centro, otorguen la formación necesaria al alumno facilitándole al mismo los conocimientos necesarios en los diferentes riesgos mencionados en la memoria.

Se pretende lograr mediante el trabajo propuesto, obtener en los centros de enseñanza en los cuales se aplique el plan educativo realizado, disminuir el riesgo al que nuestros alumnos se exponen en el uso de las nuevas tecnologías así como evitar situaciones de conflicto en la red necesitadas de tratamiento y atención.

El tutor del grupo, será el encargado del centro de enseñanza destinado a facilitar la formación a los alumnos donde se proponen sesiones de una hora en cada formación dedicada a los diferentes riesgos. Sesiones, las cuales se pueden impartir en diferentes tutorías que pueden constar de un debate en el aula por parte del grupo, de modo que se requiera la participación activa de la clase y cada alumno pueda exponer sus diferentes experiencias o dudas.

Los objetivos generales marcados de la primera sesión que los alumnos deben conocer referentes a la **privacidad y seguridad en internet son**:

- Conocimiento por parte del alumno de actividades ilícitas en la red
- Adoptar conceptos básicos en seguridad al navegar como navegar siempre de forma privada en la red (pestaña del navegador→navegar de forma privada)
- Entender la importancia y respeto de la privacidad en la red.
- Comprender que se deben realizar contraseñas seguras combinando cifras, números, mayúsculas y minúsculas.
- Riesgos que existen de la pérdida de datos personales y privacidad en la red.

Se propone para lograr el objetivo realizar las siguientes actividades:

- Realización de un debate referente a la falta o no de seguridad que implica conectarse a la cuenta de correo personal en cualquier ordenador y con cualquier conexión a internet como puede ser la conexión wifi gratuita de un centro público cualquiera.
- Planteamiento y reflexión por parte de los alumnos: ¿Si encuentro un ordenador con una cuenta de correo personal abierta que he de hacer?

Con la actividad planteada se logra, que el alumno reflexione e investigue en materia de seguridad referente a que pasos debe seguir para mantener su privacidad en la red y que realice a su vez una pequeña reflexión acerca de la conducta ética en la red. Se debatirá en el aula con todos los alumnos y alumnas asistentes en la tutoría.

4.2.1 PREVENCIÓN DEL CIBERACOSO

El ciberacoso o ciberbullying se define como acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

Las formas que adquiere el ciberbullying son de diferentes tipos, se pueden realizar envíos de mensajes ofensivos, amenazadores, denigrantes, que pretenden ridiculizar, pero también se realizan fotografías, videos, llamadas en forma de acoso, correos faltando el respeto, o páginas web donde se insulta.

Los pioneros en la investigación del ciberbullying son Li. Q. (2007)(13) y Katz (2006)(14), los cuales asocian el uso de las TIC que puede repercutir tanto en una correcta convivencia como para usos violentos.

En un análisis realizado por Belsey sobre el fenómeno del Ciberbullying, lo define como" *el uso de algunas Tecnologías de la Información y la Comunicación como el correo electrónico, los mensajes del teléfono móvil, la mensajería instantánea, los sitios personales vejatorios y el comportamiento personal en línea difamatorio, de un individuo o un grupo, que deliberadamente, y de forma repetitiva y hostil, pretende dañar otro"* (Belsey, 2005) (15).

*Los jóvenes usan weblogs, redes sociales y sistemas de mensajería instantánea para intimidar a sus compañeros, siendo la difusión de fotografías retocadas para ridiculizar a las víctimas uno de los métodos más empleados. Estas son distribuidas masivamente y a veces indicando la identidad de aquel que es sometido a la humillación para acrecentar el impacto. En el caso de las comunidades virtuales, muchas de ellas precisan de invitación para poder entrar a formar parte de un grupo, el acoso escolar se basa en aislar a aquellos que son las víctimas de las humillaciones e intimidaciones. Allí se establecen conversaciones que luego son continuadas en el centro escolar y quienes no pertenecen al grupo quedan descolgados de sus compañeros (*Fante 2005) (16).

La educación y la correcta difusión de pautas seguras de actuación son claves para otorgar a los menores, las herramientas adecuadas que garanticen un uso seguro de todas las funcionalidades de las TIC trantando de evitar en el alumno conductas referentes a ciberbullying pasivo o activo.

"Podrán corregirse, de acuerdo con lo dispuesto en este título, los actos contrarios a las normas de convivencia del centro realizados por los alumnos en el recinto escolar o durante la realización de actividades complementarias y extraescolares. Igualmente, podrán corregirse las actuaciones del alumno que, aunque realizadas fuera del recinto escolar, estén motivadas o directamente relacionadas con la vida escolar y afecten a sus compañeros o a otros miembros de la comunidad educativa." (Artículo 46, Real Decreto 732/1995, derechos y deberes de los alumnos y las normas de convivencia en el centro) (17)

El alumno en el plan educativo propuesto, debe conocer las pautas a seguir, y para ello se estima que el tutor logre con su grupo correspondiente los siguientes objetivos propuestos, que continuarán con las sesiones de una hora en cada formación dedicada a los diferentes riesgos, que como se ha comentado se pueden impartir en las diferentes tutorías.

Los objetivos generales marcados de la segunda sesión que los alumnos deben conocer referentes al **ciberacoso o ciberbullying** son:

- Recibir información sobre el ciberbullying en las tutorías por parte del docente.
- Informar al centro de enseñanza por parte de los alumnos si detectan que un compañero o en su propio caso, son víctimas de ciberbullying .
- Conocer las técnicas que utilizan los ciberacosadores, con tal de poder realizar la prevención necesaria.
- Ser conocedores de la necesidad de denunciar el acto del ciberacoso al primer síntoma de detección.
- No ofrecer información personal a desconocidos.
- Tener la constancia de que toda foto o video que se sube a internet no desparace
- Tener una conducta responsable y ética en la red, siendo conocedores de realizando aquellas actividades como suplantar identidades, calumnias, acoso, o robo de privacidad se puede incurrir en un delito
- No contactar ni citarse personalmente con desconocidos, solamente agregando como amigos aquellas personas que conocen personalmente.

Para lograr los objetivos marcados, se propone realizar una actividad, en la que el docente exponga un caso práctico referente a un alumno que sufre ciberacoso en la red por parte de sus compañeros del centro de enseñanza. De tal modo que se debatan por parte de los alumnos, las pautas previamente explicadas parte del docente de actuación ante un caso de ciberbullying.

En este caso, debatiendo en el aula por parte de los alumnos junto con su tutor cuestiones del siguiente tipo:

- ¿Por qué el alumno que sufre ciberacoso no denuncia la situación? (Ley del silencio)
- ¿Qué consecuencias sufre el alumno que es acosado?
- ¿Cómo ayudarías a un compañero que sufre ciberacoso?

Los docentes del centro, deberán estar atentos con tal de detectar posibles alertas en alumnos en determinadas situaciones de conflicto que pueden desembocar en ciberbullyng. Para ello, es recomendable lograr la confianza del grupo de alumnos por parte del tutor, de modo que los alumnos aprecien en la figura del tutor una persona a la que acudir ante cualquier conflicto.

Algunos comportamientos de los alumnos, mediante los cuales los docentes pueden detectar un signo de alerta en el alumno a este respecto son los siguientes:

- Que el rendimiento académico y la concentración del alumno disminuyan repentinamente.
- Aislamiento del alumno.

- Frecuentes dolores de cabeza, nerviosismo, dolores de estomago
- Comportamiento distante, ya no se relaciona con sus compañeros.
- Tristeza, apatía.
- Cambios de humor.

Se aconseja para el plan realizado, al menos una reunión con los padres de los alumnos, referente al ciberacoso. La figura de los padres, es muy importante a su vez para el detectar y prevenir este tipo de situaciones de ciberacoso.

Por ello, en la reunión con los padres, se debe ofrecer a las familias la información necesaria en materia de ciberacoso, de tal modo que las propias familias presten especial atención al uso de las TIC por parte de sus hijos en sus hogares, para evitar este tipo de comportamiento tanto si es activo como pasivo.

Los comportamientos en Internet no son más que un reflejo de los comportamientos en sociedad, ya que Internet permite el desarrollo de nuevas formas de relación social que no tienen su origen en Internet, sino que son fruto de una serie de cambios históricos pero que no podrían desarrollarse sin la red de redes (Castells,1999)

4.2.2 GROOMING, SEXTING

El *sexting* se basa en la publicación o difusión de contenidos como fotografías o vídeos de tipo sexual, que son producidos por el propio remitente, utilizando para tal fin el teléfono móvil u otro dispositivo tecnológico. El termino *grooming* por su parte, hace referencia al conjunto de acciones que una persona lleva a cabo sobre un menor con un objetivo sexual, mediante el cual busca la obtención de imágenes del menor en situaciones sexuales e incluso la búsqueda de establecer contacto en persona con el propio menor.

Las actividades de *grooming*, pueden llegar a ser calificadas como un delito de acoso sexual según lo estipulado en el art.184 del Código Penal: *"…El que solicitare favores de naturaleza sexual para sí o para un tercero, en el ámbito de una relación laboral, docente o de prestación de servicios, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante, será castigado, como autor de acoso sexual, con la pena de arresto de seis a doce fines de semana o multa de tres a seis meses…".(20)*

El delito se agrava en caso en que la víctima sea un menor de edad, según lo dispuesto en el art.184.3 *"…Cuando la víctima sea especialmente vulnerable, por razón de su edad, enfermedad o situación, la pena será de arresto de doce a veinticuatro fines de semana o multa de seis a doce meses en los supuestos previstos en el apartado 1, y de prisión de seis meses a un año en los supuestos previstos en el apartado 2 del presente artículo…"(20).*

Los datos referentes al Sexting arrojan los siguientes porcentajes:

- *"En España, 2 de cada 3 menores de 10 a 16 años (un 64,7%) posee un terminal de telefonía móvil propio.*
- *Este porcentaje aumenta con la edad y se generaliza entre los adolescentes (de 15 a 16 años): un 89,2% tiene teléfono móvil.*
- *El 88,6% de los menores españoles con móvil entre 10 y 16 años hace fotografías con su terminal, el 48,2% las envía a otras personas, y el 20,8% las publica en Internet.*
- *En España, un 4% de los menores entre 10 y 16 años dice haberse hecho a sí mismos fotos o vídeos en una postura sexy (no necesariamente desnudos ni eróticas) utilizando el teléfono móvil.*
- *El 8,1% de los adolescentes españoles de 10 a 16 años declara haber recibido en su teléfono móvil fotos o vídeos de chicos o chicas conocidos en una postura sexy." (INTECO, 2011)(19).*

Así mismo, la misma fuente (INTECO, 2011)(19) según el estudio de investigación realizado, aporta los siguientes datos:

- *"En el sexting, el menor es el que, conscientemente, realiza (o consiente la realización) de una fotografía o vídeo con contenido sexual y la distribuye o publica de manera voluntaria.*
- *Parece evidente que el menor no está percibiendo amenaza alguna contra su privacidad, ni es consciente de las implicaciones desde el punto de vista de la seguridad. No ven riesgos en la exposición de datos personales, privados e íntimos, a través de las nuevas tecnologías de la comunicación, y por ello los difunden. Se colocan a sí mismos en una situación de vulnerabilidad, en tanto en cuanto unos contenidos de sexting pueden llegar a ser conocidos de forma masiva.*
- *Puede ser que los adolescentes muestren tal avidez de reconocimiento y notoriedad que les lleva a mostrar cierto exhibicionismo online, lo que puede llevar a situaciones que pueden incluso poner en peligro su intimidad e integridad." (INTECO, 2011)(19).*

Se proponen lo siguientes objetivos generales marcados en la tercera sesión del plan educativo de seguridad y privacidad en la red, que los alumnos deben conocer referentes al **grooming y sexting:**

- El alumno, debe conocer los riesgos de grooming y sexting de modo que pueda prevenir este tipo de situaciones de riesgo.
- El alumno, debe entender la necesidad de solicitar ayuda a los docentes del centro de enseñanza o a la familia.

- Si un alumno realiza dicha la actividad de *grooming o sexting* a un compañero, al pertenecer al mismo centro de enseñanza, este debe de informar al centro, de modo que el propio centro de enseñanza tome las medidas disciplinarias oportunas para resolver el conflicto.
- Concienciación al alumno del riesgo de publicar fotos de contenido sexual en internet. Entendiendo que todo el material que se sube a la red ya no desaparece.
- Es muy importante que mediante la tutoría se logre trasladar a los alumnos la confianza suficiente como para que, ante un conflicto en la Red, recurran a la opinión experta del tutor o de las familias.

Se propone para lograr la concienciación por parte de los alumnos, realizar una actividad en la tutoría (previa explicación del tutor referente a *grooming y sexting)* en que los alumnos y docente debatan juntos cómo actuarían para evitar estos riesgos en la red, y en caso de sufrir *grooming* cómo actuarían para salir de tal situación.

Con dicha actividad, se pretende:

- La reflexión y concienciación por parte del alumno, estudiando los mecanismos que tiene a su disposición para evitar los riesgos.
- Lograr comprender que no se encuentra solo y puede confiar en figuras como la del educador o su familia,
- Hacer frente a las amenazas o represalias del acosador.
- Abandonar la sensación de culpabilidad.

A su vez es necesario informar a las familias por parte de los tutores, para que estén atentos al uso que sus hijos hacen de los ordenadores y teléfonos móviles (igual que en el caso anterior). De modo que se pueda lograr evitar este tipo de riesgo en el menor.

4.3 LAS REDES SOCIALES: TÉCNICAS PARA LA PRIVACIDAD Y SEGURIDAD DE LOS ALUMNOS

Las redes sociales, en los adolescentes, pueden derivar en un uso adictivo no siendo capaces de controlar el tiempo que pasan conectados a las mismas debido a una sensación donde disfruta más conectado en el mundo virtual que en el propio mundo real. *En el caso de los adolescentes, las conductas adictivas en este ámbito pueden ponerse de manifiesto cuando la tecnología pasa de ser un medio a convertirse en un fin en sí misma; por ejemplo, cuando se siente una obsesión enfermiza por disponer siempre del móvil de última generación, o cuando un adolescente queda atrapado en las redes sociales de Internet porque en el mundo virtual puede disfrutar de una identidad falsa e irreal* (Becoña, 2006) (21)

Se puede definir una red social como un aplicativo que permite a los usuarios, crear un perfil público, colaborar en la edición de contenidos, compartir información, o participar en determinados movimientos de la sociedad. Creando para el usuario una extensión de sus relaciones sociales, en la cual se mantienen o crean contactos con amigos, conocidos y se comparten con ellos información, videos, juegos o fotografías.

Uno de los problemas de las redes sociales, es la adicción que provoca en los adolescentes siendo mayor que en los adultos.*Probablemente, el mayor riesgo del uso excesivo de las nuevas tecnologías es la posibilidad de generar un comportamiento adictivo que lleve no solo a una dedicación desmedida (lo que puede apartar al chico o chica de otro tipo de actividades más saludables y muy necesarias a ciertas edades), sino a una verdadera dependencia y falta de control sobre sus conductas. Esta adicción es más probable que se genere en el adolescente que en el adulto, debido a que su corteza prefrontal se encuentra aún inmadura y su autocontrol no ha alcanzado aún el nivel adulto* (Oliva, 2007) (22).

Los principales riesgos de las redes sociales son (23):

- *Protección de Datos de Carácter Personal.*
- *Protección de la Privacidad, Honor, Intimidad y Propia Imagen.*
- *Protección de la Propiedad Intelectual e Industrial.*

En referencia a las redes sociales, se proponen lo siguientes objetivos generales marcados en la cuarta sesión del plan educativo de seguridad y privacidad en la red, que los alumnos deben conocer:

- Concienciación y formación de los alumnos, mediante dialogo en la tutoría y fuera de ella, informando de los riesgos que conllevan las redes sociales.
- Entender que un uso continuado de las redes sociales pueden desembocar como se ha comentado previamente en una conducta adictiva.
- La importancia de mostrar una conducta ética y de respeto con el resto de usuarios de la red social.
- No llevar a cabo actos que puedan vulnerar la intimidad de los usuarios de la red social.
- Deber de denunciar y solicitar en la propia red social la retirada de un video o fotografía en los que aparezca el alumno de modo que sean eliminados inmediatamente, al no existir permiso autorizado para su publicación.

Algunas técnicas que los alumnos deben conocer son las siguientes:

- Evitar relacionarse con desconocidos y evitando a su vez el envío de información privada a los mismos así como fotografías y/o videos.
- Evitar facilitar datos personales en la red social mediante los cuales se pueden identificar a la persona o su familia (como dirección, teléfono).
- Uso de un perfil restringido de modo que únicamente puedan acceder al mismo aquellas personas que son conocidas a familiares del alumno,
- Evitar confrontaciones, en muchos casos de mensajes hirientes donde lo mejor es denunciar a la red social dicho comportamiento por parte de otro usuario.

La protección de la privacidad en las redes sociales no es la adecuada, siendo las redes sociales un campo especialmente vulnerable para la privacidad (Antoni Roig, 2009) (24) por ello las medidas mencionadas pueden ser de gran utilidad para el alumno.

Así mismo, se plantea una actividad, a realizar en la tutoría, en la que se plantee un caso, referente a un alumno que sufre una suplantación de identidad en una determinada red social por otro alumno del aula que se hace pasar por él, suplantando su identidad. Y a su vez realizando todo tipo de comentarios hirientes que tratan de ridiculizar y desprestigiar la reputación del compañero afectado.

Con la actividad propuesta se pretende poner a prueba por parte del alumno la capacidad de empatía, situando al alumno en una posición incómoda, de tal modo que reflexione referente al daño que causan determinados comportamientos no éticos en una red social. Observar la capacidad de resolución del alumno, enfrentándose a una situación desconocida, adaptando los mecanismos previamente explicados referente a las denuncias en las redes sociales. Y la percepción del peligro que pueden acarrear determinados comportamientos en las redes sociales.

Lo que se pretende es transmitir al alumno, la importancia del buen uso seguro y responsable de las Tecnologías de la información y de la comunicación.

5. MEDIDAS DE SEGURIDAD AVANZADAS A IMPLANTAR DESDE EL DEPARTAMENTO DE SI/TI DEL CENTRO DE ENSEÑANZA.

Las medidas de seguridad que a continuación se mencionan, son como reza el título, medidas a implantar desde el departamento de sistemas y tecnologías de la información del centro.

Son medidas que he considerado de necesaria implantación en los centros de enseñanza fruto de mi experiencia en las prácticas del máster.

En el papel de observador en las prácticas realizadas del máster (primera fase del Prácticum, observación del aula), he observado que muchos alumnos tenían instalados en sus portátiles juegos de ordenador a los cuales al mínimo despiste del profesor, arrancaban el juego para seguir sus partidas. De esta observación la propuesta a implantar que logra mejorar la concentración de los alumnos en la formación academica es la siguiente:

- Sistemas operativos en los portátiles de los alumnos preinstalados en que los alumnos no puedan ejecutar comandos como root, impidiendo que instalen nuevo software lo que incluyen videojuegos.

En muchos casos, es el propio centro de enseñanza, el que realiza la venta de los ordenadores portátiles al alumno, por lo que el centro puede solicitar al proveedor, que los ordenadores estén del modo mencionado. Con ello, se evitaría que los alumnos utilizaran el portátil con otros fines que no fueran educativos.

Los alumnos, durante las clases, he podido visualizar también en el Prácticum como accedían a determinadas páginas web que nada tenían que ver con la materia que se impartía. Por lo que una medida de seguridad a adoptar por el departamento de sistemas y tecnologías de la información del centro es la siguiente:

- Restringir el acceso en el centro de enseñanza a páginas de internet no destinadas a fines educativos.

Es sencillo, ya que existen multitud de aplicaciones donde por medio del servidor se puede controlar el acceso a determinadas páginas web, tanto seleccionando solamente las páginas que se pueden acceder como restringir páginas web según su temática. Por ejemplo evitar la conexión a las redes sociales como Twitter o Facebook, o citando otro ejemplo, evitar la conexión a páginas de videojuegos.

Mencionar que se puede otorgar acceso libre a la web a los docentes del centro de enseñanza sin restricción a la vez que se realiza la restricción de páginas web a los portátiles de los alumnos.

Para el correcto uso de la información por parte de los ordenadores de los miembros de la comunidad educativa del centro de enseñanza, se mencionan siguientes medidas a implantar por el departamento de sistemas y tecnologías de la información del centro:

- Limitar el acceso del usuario, exclusivamente a las carpetas del servidor que sean necesarias para desempeñar su trabajo, de modo que no pueda acceder a documentación que no le atañe.

- Prohibir el uso de herramientas de conexión remota a los ordenadores del centro de enseñanza. Se realizará por medio de políticas en el servidor, permitiendo solamente que usuarios autorizados previamente puedan hacer uso de conexiones remotas.

- Obligación de activar un salvapantallas de modo que se active al cabo de unos minutos cuando el usuario no haga uso de su equipo, de tal modo que solicite contraseña y evitando así que otro usuario pueda acceder a su ordenador.

- Limitar las propiedades avanzadas del sistema operativo, de modo que el usuario no pueda cambiar la configuración, únicamente bajo autorización del administrador de sistemas.

- Prohibir el acceso a redes externas que no sean las establecidas por el departamento de tecnologías de la información.

- Si el usuario del centro de enseñanza necesita copiar archivos de carácter personal a un dispositivo móvil o un ordenador portátil, deberá solicitarlo previamente al departamento de SI/TI del propio centro de enseñanza.

- En caso de creación de un fichero propio de datos de carácter personal deberá solicitar la autorización correspondiente

6. PLAN DE CONVIVENCIA DEL CENTRO EN MATERIA DEL USO DE RED Y LAS NUEVAS TECNOLOGÍAS.

Se proponen dentro del plan que se está realizando, unas indicaciones en materia de nuevas tecnologías de modo que se reflejen en el plan de convivencia del centro de enseñanza, por medio de las normas de comportamiento y reglamentos oportunos en la materia.

- ✓ **Uso responsable y seguro de las TIC:** El centro debe promover el uso responsable y seguro de las TIC en los alumnos del centro de enseñanza.

- ✓ **Información y colaboración con las familias:** El centro educativo debe informar a las familias en referencia al correcto uso de las TIC. De modo que colaboren con el centro de enseñanza en seguir las directrices marcadas por el propio centro para lograr el correcto proceso educativo en formación en la seguridad de los alumnos en la materia.

- ✓ **Respeto a los alumnos y personal del centro de enseñanza:** No se permite difundir en las redes sociales y por ende internet, ningún tipo de imagen, foto o video de cualquier miembro de la comunidad educativa del centro.

- ✓ **Protección de la imagen del alumno**: Los alumnos y alumnas del centro de enseñanza, deberán evitar subir imágenes propias e información que los pueda identificar a las redes sociales sin el permiso de la familia.

- ✓ **Restricción del uso de los móviles:** No se permite el uso de dispositivos móviles en horario escolar, a excepción de autorización específica de un profesor por una causa o motivo completamente justificado.

- ✓ **Asesoramiento y apoyo del centro de enseñanza al alumno en conflictos derivados de las TIC:** El centro de enseñanza, ante cualquier conflicto, falta de respeto o acoso en materia de las tecnologías de la información y comunicación, apoyará y asesorará al alumno tomando las medidas oportunas para la resolución del conflicto.

- ✓ **Inculcar al alumno comportamientos adecuados en el uso de las redes sociales:** El centro debe fomentar valores a sus alumnos en el correcto uso de las redes sociales, de modo que se eviten riesgos y todas aquellas actividades que ponen en riesgo al alumno como la suplantación de identidad, acoso, robo de datos, o la adicción.

Con el decálogo mencionado se trata de adaptar el trabajo realizado referente al plan educativo en seguridad, de modo que se reflejen las actividades referentes al uso responsable y seguro de las TIC, en el plan de convivencia del centro de enseñanza.

7. RESULTADOS

Durante mi permanencia en el centro, en la realización del Prácticum, he podido verificar la necesidad de realizar un plan educativo de seguridad y privacidad en la red para el beneficio de la comunidad educativa del centro de enseñanza.

Una vez reunido en el propio centro de enseñanza con mi tutor del trabajo final de máster y mi coordinadora de las prácticas del máster, se decidió que la propuesta era muy buena, donde se debía orientar a un enfoque a su vez pedagógico y no solamente de carácter técnico.

Solicité también opinión al responsable del departamento de informática del centro, y la propuesta le pareció viable a la vez que interesante.

Con el resto de profesores y compañeros del departamento de tecnología que les comenté el trabajo, me mostraron su satisfacción, encontrando el trabajo realmente útil y adaptado al momento de auge tecnológico que vivimos en la actualidad en el que la tecnología de la información está tan presente en nuestro entorno diario.

Una vez realizado el trabajo, se pueden obtener unos resultados que impactan en varias áreas del centro de enseñanza, ya que es un trabajo completo en el que se logran los siguientes resultados:

- ➢ Aplicación de normativas de privacidad y protección de ficheros en el centro de enseñanza, cumpliendo con la Ley Orgánica de Protección de datos.

- La aplicación de las normas de protección de datos y privacidad en los centros escolares

- Alumnos formados en el uso responsable y seguro de las TIC.

- Prevención del ciberacoso : ciberbullying

- Prevención del ciberacoso : sexting y grooming

- Centro de enseñanza que logra un valor añadido para los alumnos y familias al mostrar su compromiso, responsabilidad y formación en el uso seguro de las TIC en los estudiantes del centro.

- Docentes con mejor formación tecnológica en materia de seguridad y privacidad de las TIC

- Docentes capaces de establecer ayuda y asesoramiento a sus alumnos en situaciones conflictos en materia de seguridad mediante la introducción de contenidos de seguridad y prevención en el plan de acción tutorial.

- Plan de Convivencia del Centro adaptado al uso de las Nuevas tecnologías

- Mayor productividad y concentración del alumno en el centro de enseñanza. Debido a la implantación de medidas de seguridad avanzadas desde el departamento de sistemas de información del propio centro que logran evitar distracciones como accesos a páginas web inapropiadas o la instalación de juegos en los portátiles de los alumnos.

Con los resultados obtenidos, se desprende la realización de un trabajo que ha pretendido repercutir en las diferentes áreas implicadas en materia de seguridad y privacidad en la red de un centro de enseñanza.

8. CONCLUSIONES

La seguridad y privacidad de la información, así como el uso responsable y seguro de las TIC, es uno de los retos actuales que plantea el mundo educativo.

Algunos de los propósitos marcados, han sido dotar al centro de enseñanza, de los mecanismos para hacer frente a los diferentes riesgos de los alumnos en la red como el ciberacoso, o resolver conflictos en la red, conociendo la legislación sobre los menores, e implantar medidas de protección de datos, privacidad y seguridad en beneficio de los alumnos y centros de enseñanza.

El título del TFM *"Plan estratégico educativo de seguridad y privacidad en la red para alumnos y docentes en los centros de enseñanza*" define claramente la propuesta realizada en el uso seguro de las TIC desarrollando e implementando una solución a esta problemática.

Durante la realización del trabajo, he tratado de realizar un enfoque más pedagógico, y evitando el uso de tecnicismos o medidas de seguridad muy técnicas que conozco como graduado en ingeniería informática.

En determinados puntos de la memoria, se aprecia la necesidad que en este ámbito de la seguridad y la privacidad en la red, sean participes tanto los miembros de la comunidad educativa que forman el centro, como los alumnos y la familia.

He dedicado una pequeña parte de la memoria en relación a medidas a implementar por el departamento de informática del propio centro de enseñanza, ya que he estimado estas medidas como imprescindibles, las cuales noté a faltar en el instituto donde realicé las prácticas del máster. Son medidas que logran un aumento de la productividad del alumno. Evitando todo tipo de distracciones y que facilitan al docente su trabajo al no tener que estar pendiente de que el alumno se despiste por ejemplo accediendo en horario lectivo a determinadas páginas web que no tienen nada que ver con la materia.

La documentación obtenida en la materia del proyecto, fruto de la investigación para la realización del trabajo, me ha permitido adquirir unos valiosos conocimientos que aportan un valor añadido a mi currículum profesional al haber realizado un amplio aprendizaje en seguridad en la red y protección de los alumnos en los centros de enseñanza. Y lo más importante, es que son muy valiosos en cualquier comunidad educativa para el beneficio del centro de enseñanza.

9. BIBLIOGRAFÍA Y WEBGRAFÍA

(1)Investigación sobre conductas adictivas a Internet entre los adolescentes europeos. Informe realizado por EU NET ADB Consortium, 2013 (Recopilación de datos Octubre 2011- Mayo 2012). Disponible en
http://www.eunetadb.eu/files/docs/FinalResearchInternet-ES.pdf

(2) Currículum educació secundària obligatòria – Decret 143/2007 DOGC núm. 491
Disponible en:
http://www.xtec.cat/alfresco/d/d/workspace/SpacesStore/52b74b46-424a-4a4e-9338-a32e5a3a81c3/competencies_eso.pdf

(3) Mark Griffths,1995 Technological addictions. Clinical Psychology Forum, 76, 14-19

Disponible en:
http://www.academia.edu/751805/Griffiths_M.D._1995_._Technological_addictions._Clinical_Psychology_Forum_76_14-19

(4) Mariano Chóliz, Profesor de la Facultad de Psicología Básica de la Universitat de València (UV).

(5) *El ciberacoso como forma de ejercer la violencia de género en la juventud; Un riesgo en la sociedad del de la información y el conocimiento.* Ministerio de Sanidad, Servicios Sociales e Igualdad
(Informe de 2013)
Disponible en:
http://www.msssi.gob.es/ssi/violenciaGenero/laDelegacionInforma/pdfs/Ciberacoso_Adolescencia.pdf

(6)Adolfo Sánchez Burón, Adolfo Álvaro Martín.Universidad Camilo José Cela ."*Hábitos de usos de las redes sociales en los adolescentes de España y América Latina"*
(Informe 2011)
Disponible en:
http://www.slideshare.net/ucjc/generacin-20-2011-hbitos-de-usos-de-las-redes-sociales-en-los-adolescentes-de-espaa-y-amrica-latina

(7) *Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles.* INTECO.
(Informe de 2011)
Disponible:
http://www.inteco.es/pressRoom/Prensa/Actualidad_INTECO/Estudio_Smartphones_Orange

(8) Constitución Española Titulo I, De los derechos y deberes fundamentakes, Capítulo II, Artículo 18.
Disponible:
http://www.laconstitucion.es/1978/19/articulo-18/3/titulo-i/de-los-derechos-y-deberes-fundamentales

(9) Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
Disponible:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/Sentencia292.pdf

(10) Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de Carácter Personal.
Disponible:
http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

(11) Disposición adicional vigesimotercera. Datos personales de los alumnos. Ley Orgánica 2/2006, de 3 de mayo, de Educación.
Disponible:
http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

(12) Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres. (INTECO, 2009)
Disponible:
http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf

(13) Li, Q. (2007). "New bottle but old wine: A research of cyberbullying in schools Computers", Human Behavior 23 , 1771-1791.

(14) Katz, J. E. (2006). Magic in the air: Mobile communication and the transformation of social life. New Brunswick, NJ: Transaction Publishers

(15) Belsey, B. (2005). Cyberbullying: An emerging Threta to the always on generation .
Disponible en:
http://www.cyberbullying.ca [consulta 2006, 20 de febrero]

(16) Fante, C. (2005). Fenómeno Bullying. *Como prevenir a violência nas escolas e educar para a paz*. Brasil: Verus.

(17) Artículo 46, Real Decreto 732/1995, derechos y deberes de los alumnos y las normas de convivencia en el centro.
Disponible:
http://www.boe.es/diario_boe/txt.php?id=BOE-A-1995-13291

(18) Castells,M.(1999). Internet y la Sociedad red*. Lección inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento (UOC)*
Disponible en:
http://www.forum-global.de/soc/bibliot/castells/InternetCastells.

(19) Guía sobre adolescencia y sexting: qué es y cómo prevenirlo. (INTECO,2011)
http://www.sexting.es/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf.

(20) Ley Orgánica 10/1995, 23 de noviembre, del Código Penal.7

(21) Becoña, E. (2006). Adicción a nuevas tecnologías. La Coruña: Nova Galicia Edicións.

(22) Oliva, A. (2007). Desarrollo cerebral y asunción de riesgos durante la adolescencia. Apuntes de Psicología, 25, 239-254.
Disponible:
www.apuntesdepsicologia.es/index.php/revista/article/download/77/79

(23) Guia sobre las Redes Sociales, menores de edad y privacidad en la red (INTECO, 2008)
Disponible:
http://www.inteco.es/guias_estudios/guias/guiaManual_redes_menores

(24) Antoni Roig (2009) Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales. E-privacidad y redes sociales.
Disponible:
http://www.uoc.edu/ojs/index.php/idp/article/viewFile/n9_roig/n9_roig_esp?origin=publication_detail